Integrated Cryptographic Hardware Engines on the zSeries Microprocessor

IBM Corporation

Jeffrey A. Magee

Thomas S. Fuchs

Seth R. Greenspan

Thomas Koehler

Bernd Nerz

Timothy J. Slegel

IBM @server

Overview

- Cryptography and Applications
- Evolution of Mainframe Cryptographic Hardware
- Implementation on zSeries Microprocessor
- Design Decisions
- Performance and Technology
- Extensible Architecture
- Summary

Cryptography

- What is it?
  - The area of mathematics and science involved in developing algorithms and methods of protecting information
- Data and Keys and Algorithms
  - Data and Key are input to a function that results in some output. Output can not be restored to original data without the proper Key
  - Symmetric and Asymmetric algorithms

Applications

- To protect information
  - From outside attackers
  - From inside attackers
- To allow secure transmission of data across unsecured channels

Applications

- Public Key Architecture (SSH/SSL) requires three services:
  - Asymmetric cryptographic algorithm
  - Secure hashing function
  - Symmetric cryptographic algorithm

SSL/SSH Startup

- Asymmetric algorithm
  - One time startup cost per session
  - Session key for symmetric crypto sent encrypted with public key of receiver
  - Receiver uses the corresponding private key to retrieve the session key from this encrypted message

SSL/SSH Session

- Symmetric algorithm and hashing
  - Session is largely composed of symmetric encryption/decryption (DES, RC4, AES)
  - Each transmission is authenticated with a secure hash function (SHA-1, MD5)

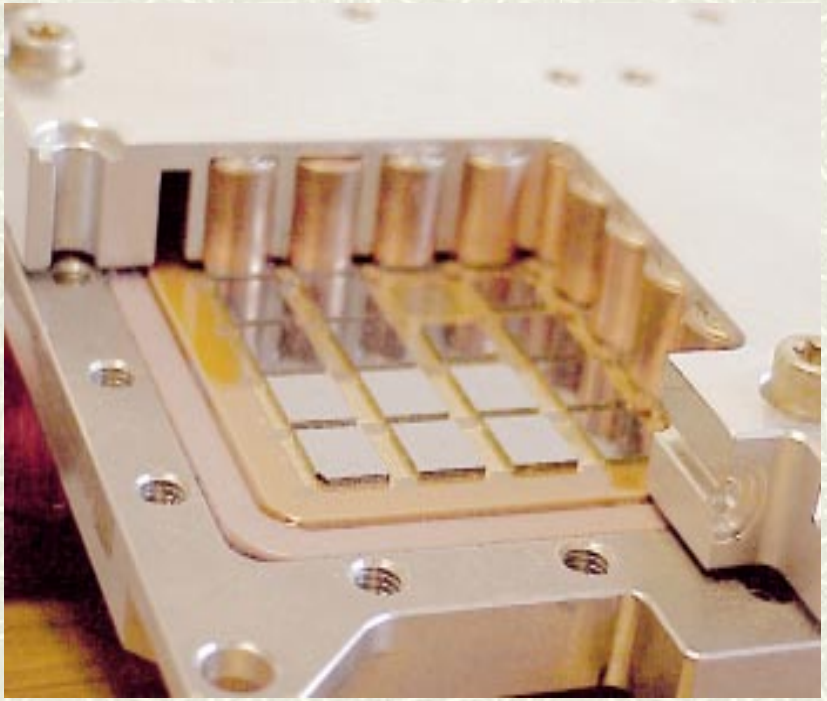
Evolution of Cryptographic Mainframe Hardware

- ES/9000 9021 ICRF
  - Only supported DES, MAC and PIN
  - External Key Storage Unit
  - Water cooled bipolar logic
  - Multi-chip Module attached to Central Processor Board

ICRF

Key Storage Unit

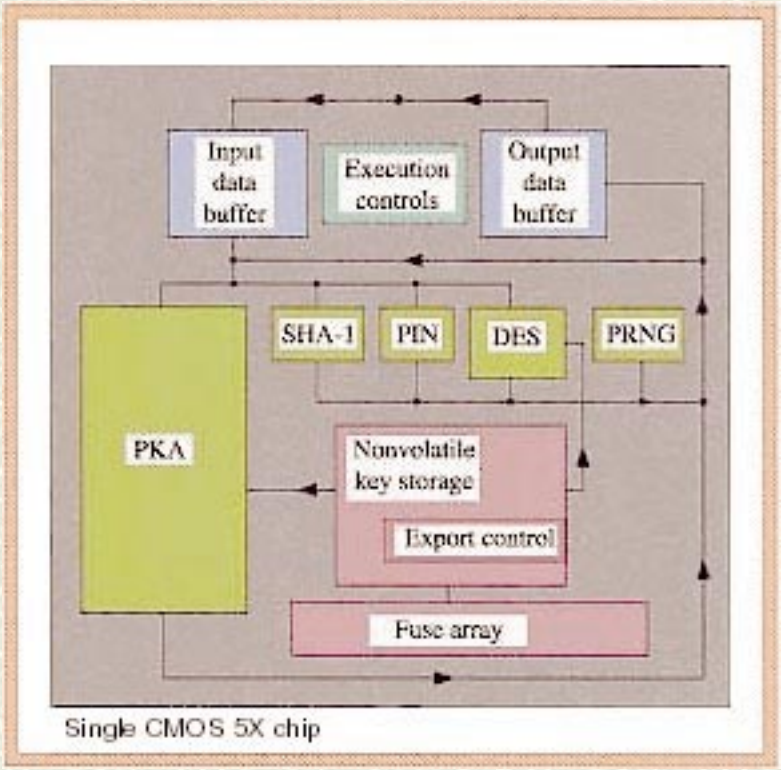
Water Cooled MCM



Evolution of Cryptographic Mainframe Hardware

- S/390 G3-G6, z900 CMOS Cryptographic Coprocessor
  - Public Key Architecture support
    - Public Key Algorithms (RSA/DSS/DH)
    - Symmetric Algorithms (DES/TDES)
    - MAC, SHA-1, PIN, PRNG
  - FIPS 140-1 Level 4 Secure
  - Single chip solution (127 MHz in G6)

Single Chip Crypto Coprocessor



Single CMOS 5X chip

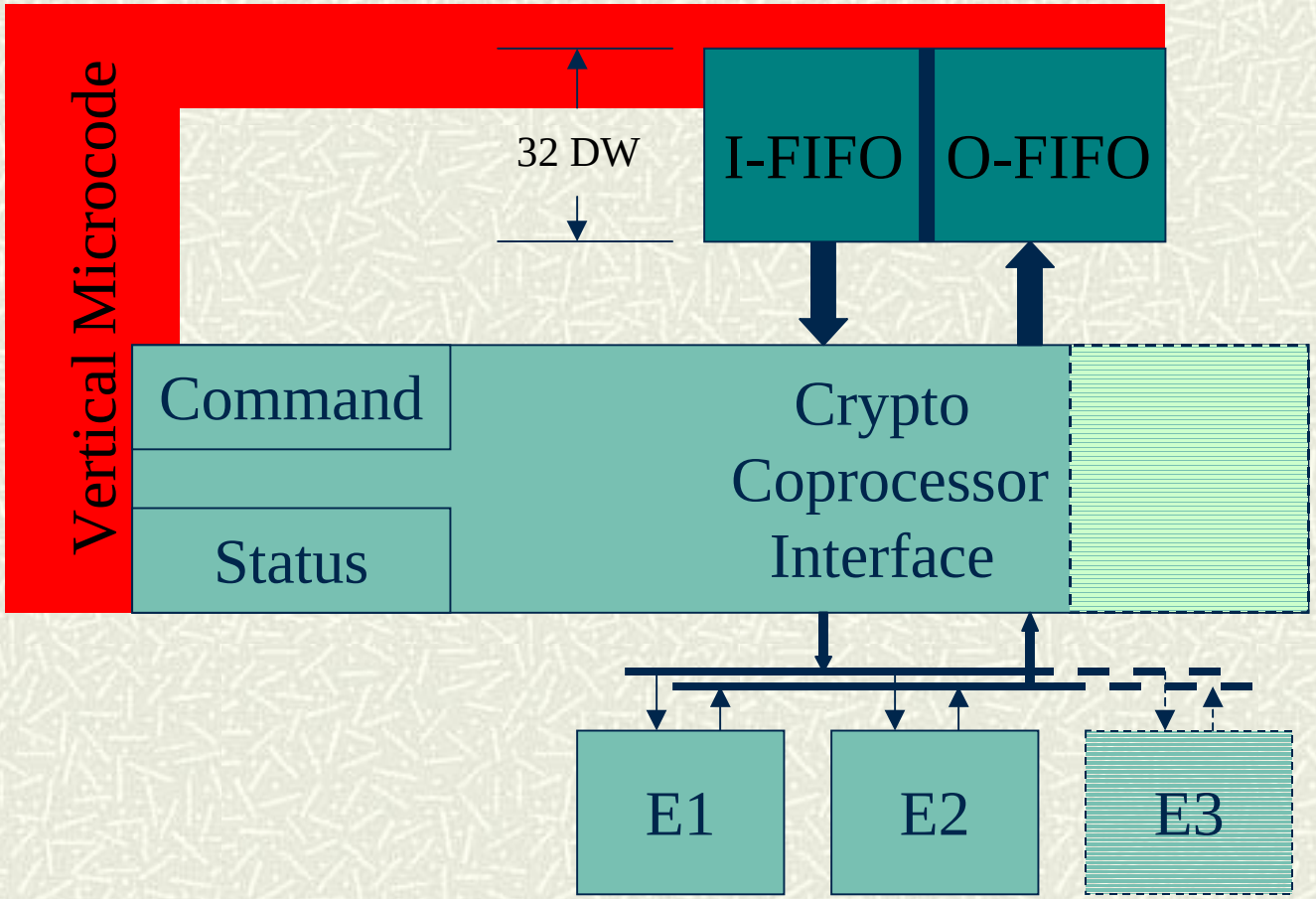
The Next Step

- As with Caches, performance increases as frequently accessed objects are located closer to the processor
  - Symmetric Algorithms (DES/TDES)
  - Hashing (MAC/SHA-1)
  - At full processor speed (>1 GHz)

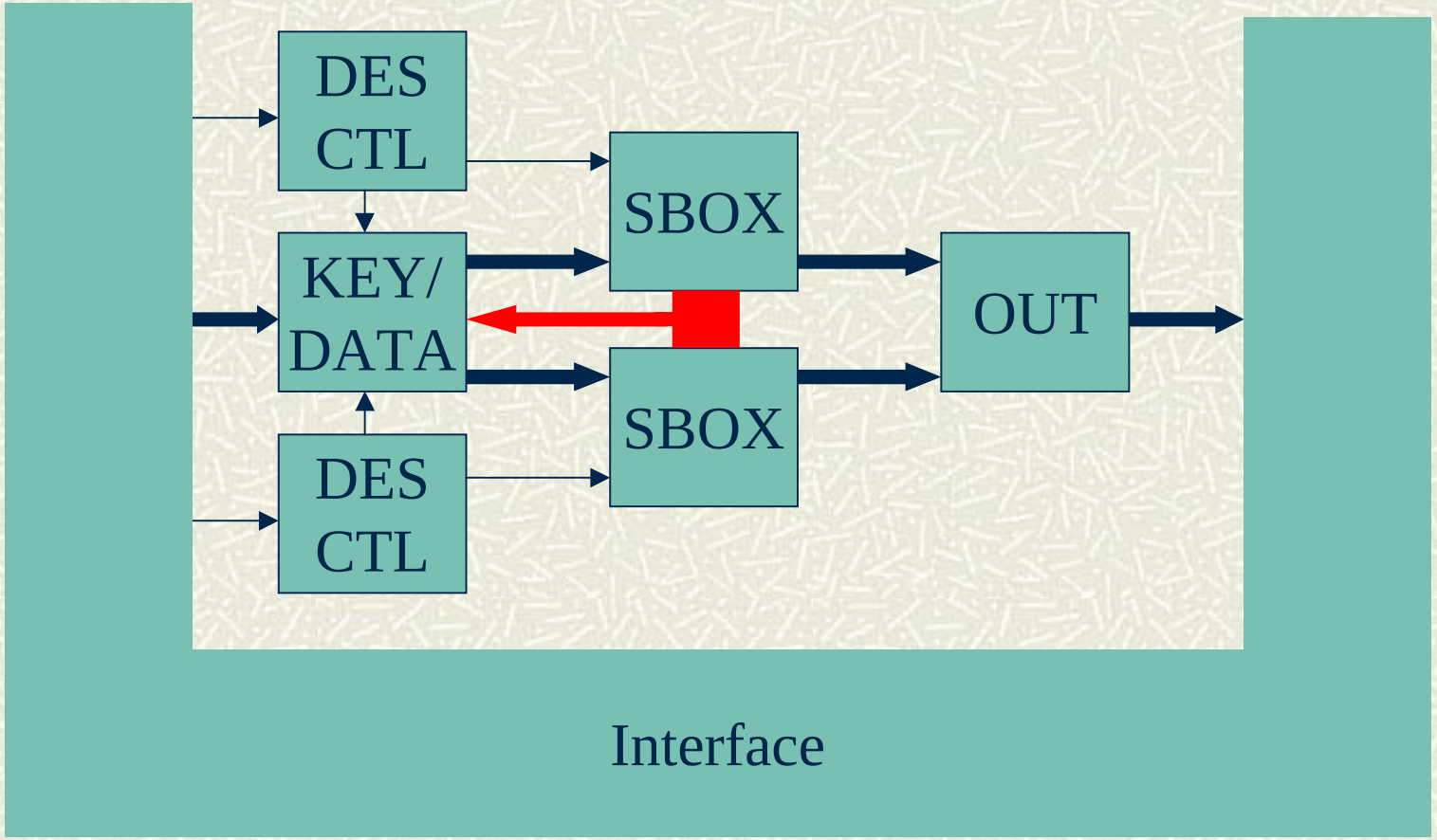
Implementation

- Data fed from 256KB Cache
- 32 Double Word deep buffers for I/O
- Control Register
- Status Register
- Vertical Microcode support

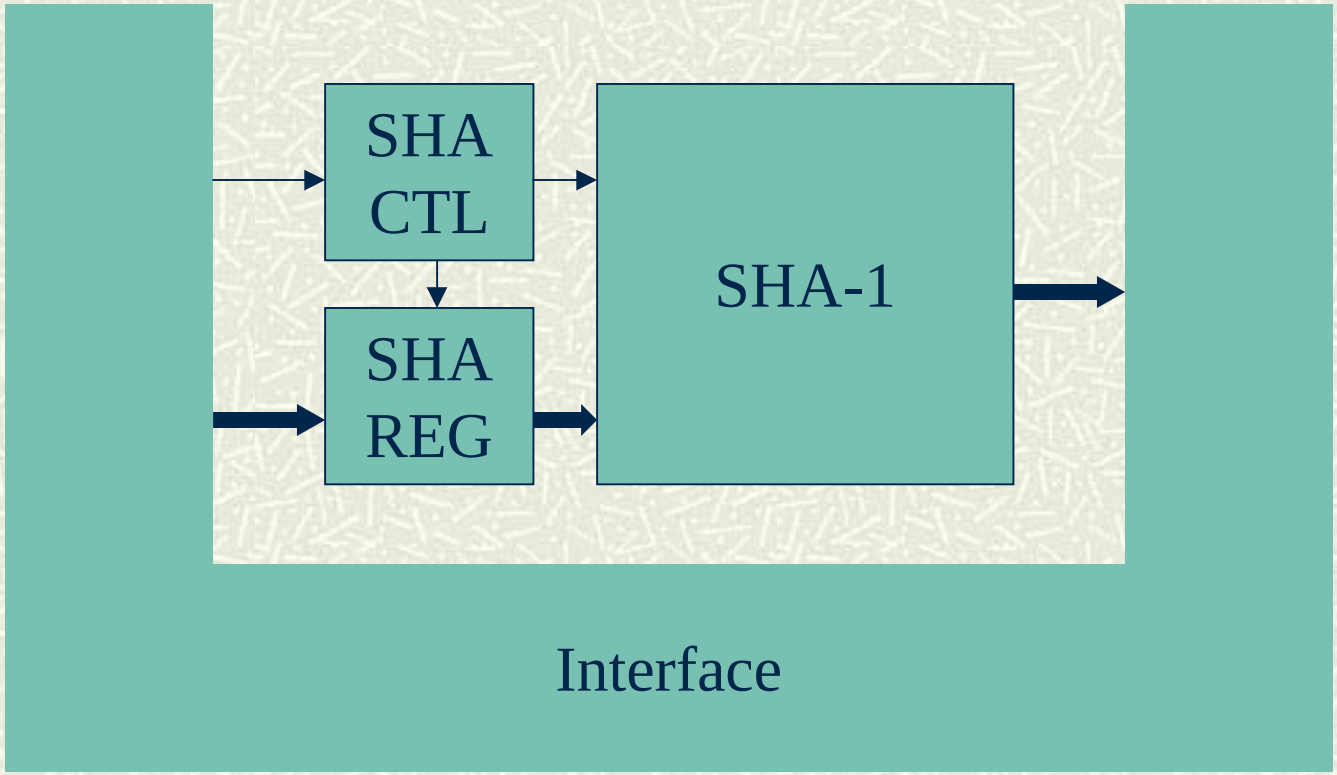
Dataflow


Vertical Microcode
32 DW
I-FIFO
O-FIFO
Command
Status
Crypto
Coprocessor
Interface
E1
E2
E3

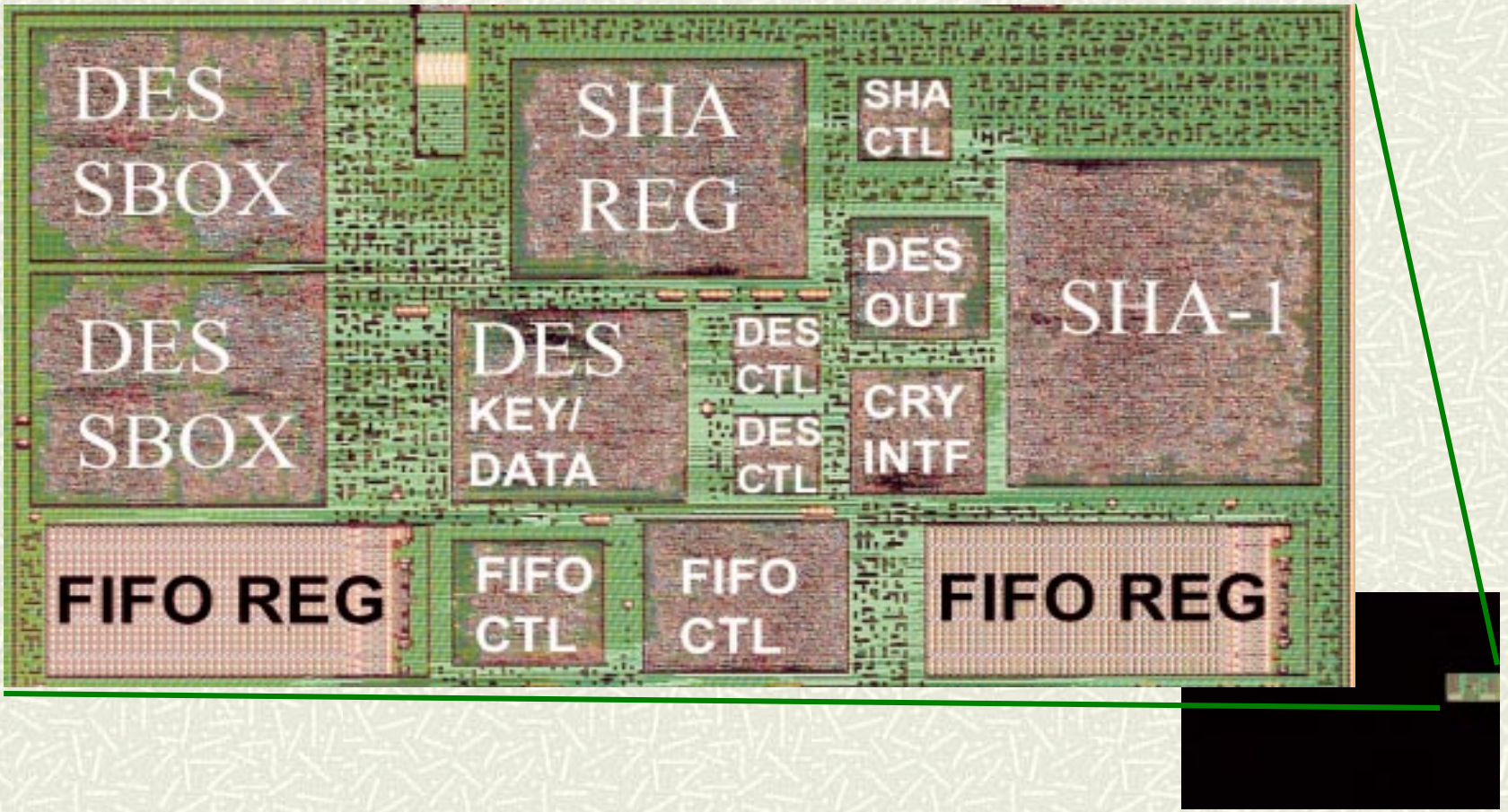
DES Microarchitecture



SHA Microarchitecture



Micrograph


DES SBOX
SHA REG
SHA CTL
DES OUT
SHA-1
DES SBOX
DES KEY/ DATA
DES CTL
DES CTL
CRY INTF
FIFO REG
FIFO CTL
FIFO CTL
FIFO REG

Design Decisions

- Selecting what belongs in the CPU
  - Asymmetric algorithms have large area requirements, and longer critical paths
    - Less frequently called
  - Hashing and Symmetric algorithms
    - More applications
    - Less overhead

Design Decisions

- Which hashing function?
  - SHA-1
    - Public domain government standard
- Which symmetric algorithm?
  - DES
    - Widely deployed, large installed base
    - TDES fulfills security requirements
  - AES
    - Not standardized in time for this design

Performance

- Single Key DES: 3.2 Gbit/s throughput
- SHA-1 Engine: 2.56 Gbit/s
  - Novel algorithm with only 2 32-bit adds/cycle
- At 1GHz…
- Cryptographic engine physical design timing indicates dataflow will support 1.4GHz operation
- We were able to partition the logic and achieve this from a fully synthesized design

Technology

- .13 micron SOI
- 8 metal layers (with copper)
- Area: 2mm^2 of 130mm^2 core
- Power saving features
  - Engines not in use can be shut down
  - Interface and IO Buffers disabled when Coprocessor not in use

Mainframe Class Reliability

- zSeries Fail Detection and Recovery
  - System has to have ability to detect and then handle error conditions gracefully
  - When error conditions arise, operation is restarted from a clean checkpointed state
  - Hard errors detected in a processor unit cause that processor's last known good state to be transferred to an alternate processor

Reliability for Crypto

- Parity prediction for SHA-1 dataflow
- DES presents a challenge for parity
  - Parity is present at data input and output
  - Prediction would impair cycle time of the ciphering dataflow
  - Solution: Duplication of dataflow and compare results
  - DES control logic also duplicated

Architecture

- Opcodes specify which type of operation
  - Example: ECB, CBC, Hash
  - Corresponding Vertical Microcode begins execution on main processor
- Function Codes for selecting:
  - Encrypt/Decrypt
  - Algorithm
  - Key Lengths

Architecture

- Vertical Microcode responsibilities:
  - Loads/Stores between FIFOs and D-Cache
  - Preprocessing (i.e. block padding)
  - Monitoring status of interface for error or operation completion
  - Interrupt polling and resuming interrupted operation

Extensible Architecture

- Architecture defines function codes for available operations
  - Up to 256 functions codes can be defined per opcode
- To add new algorithm:
  - Include hardware engine (if required)
  - Implement any required support in Vertical Microcode
- Potential for new operations using existing hardware engines (i.e. PRNG – Pseudo Random Number Generator)

Summary

- Cryptographic engines within the CPU are a feature we anticipate other platforms will need to adopt in the future
  - As more and more information is encrypted and decrypted the advantage of hardware over software solutions is clear
  - The functions need to be available with minimal latency to handle short operands as efficiently as terabytes of data